

UNITED STATES PATENT APPLICATION

FOR

DELTA CRL ENHANCEMENT

Inventors:

Michelle Zhao

Prepared by:
WAGNER, MURABITO & HAO, LLP
Two North Market Street
Third Floor
San Jose, California 95113
(408) 938-9060

1
2
3
4
5 **DELTA CRL ENHANCEMENT**

6
7
8
9 **FIELD OF THE INVENTION**

10 This invention relates generally to the field of digital certificates and
11 certificate revocation lists (CRL). More particularly, this invention relates to creation
12 of a delta CRL that spans changes over more than two CRLs.

13
14 **BACKGROUND OF THE INVENTION**

15 Digital certificates are in wide use on the Internet and in the field of
16 electronic commerce for authentication of all sorts of electronic transactions. In
17 general, such digital certificates are used to certify the identity of an entity in the
18 digital world, particularly as defined by the public key infrastructure (PKI). As digital
19 certificates are issued and used, they often are either revoked or expire after a
20 predetermined amount of time. In other situations, a digital certificate may be
21 revoked or placed on hold pending some event. In order for digital certificates to
22 be useful, it is important that those entities using digital certificates to authenticate
23 the identity of an entity presenting the digital certificate have confidence that the
24 digital certificate is valid. Generally, the validity of a digital certificate can be
25 determined by reference to a Certificate Revocation List (CRL) produced by an
26 authority that generates the certificates (usually a Certificate Authority).

27 **FIGURE 1** depicts a simple exemplary computer network 100 that utilizes
28 a digital certificate and a Certificate Revocation List. In system 100, a user terminal
29 104 may request via a network (for example the Internet) 108, a digital certificate

1 from a Certificate Authority 112. The Certificate Authority 112 generates and issues
2 the certificate, which is returned to the user terminal 104. The user terminal 104
3 can then utilize the digital certificate to carry out the transaction with another entity
4 such as remote server 116. Such transactions may include financial transactions
5 or any other transaction in which the identity of the user terminal 104 should be
6 reliably authenticated.

7 When user terminal 104 sends the digital certificate to remote server 116,
8 the remote server 116 can inspect the digital certificate against a list of revoked
9 certificates (the Certificate Revocation List) stored by the remote server 116. In the
10 event remote server 116 has not obtained a recent CRL, one can be requested from
11 the Certificate Authority 112. Certificate Authority 112 then either generates a new
12 CRL or sends the most recently generated CRL to the remote server 116. Remote
13 server 116 can then determine whether nor not the digital certificate sent by user
14 terminal 104 is valid. Thus, remote server 116 can authenticate the user terminal
15 104 and determine whether or not to authorize particular transaction at hand.

16 **FIGURE 2** depicts a message flow diagram 200 for the transaction just
17 described. In this message flow diagram, a certificate request 204 is sent from the
18 user terminal 104 to the Certificate Authority 112. The Certificate Authority 112
19 generates a certificate at 208 and returns the certificate at 212 to the user terminal
20 104. The user terminal 104 can then submit a transaction using the certificate at
21 218 to the remote server 116. Remote server 116 can then request a new CRL at
22 222 of the Certificate Authority. The Certificate Authority 112 then generates or
23 retrieves a CRL at 226 and sends the CRL to the remote server 116 at 230.
24 Depending on the nature of the transaction, the remote server 116 may process the
25 CRL at 232 by taking various actions including, for example, sorting, filtering or
26 reformatting the CRL and storing information in its own database. At 234, the
27 certificate can be authenticated against the CRL data at the remote server 116. At
28 238 the transaction can be either approved or rejected in accordance with the
29 authentication at 234 and at 242 the approval or rejection can be confirmed with the
30 user terminal 104. Those skilled in the art will recognize that many other message

1 flows are possible with the message flow 200 if **FIGURE 2** being intended as
2 exemplary of a simple use of a digital certificate and a Certificate Revocation List.

3 With reference to **FIGURE 3** the Certificate Authority 112 may generate the
4 Certificate Revocation List in accordance with process 300. CRLs are generated
5 at the Certificate Authority either on a periodic basis, or as a result of some event
6 such as a certificate revocation, or some combination thereof. The process starts
7 at 302 after which a database of certificates is queried for certificates meeting a
8 particular criteria of inactivity. One example is for the query to request all
9 certificates that have been revoked. Other certificates are assumed to still be valid
10 and active.

11 At 304 the certificate database at the Certificate Authority responds to the
12 query with certificates meeting the specified criteria. Header information is then
13 generated, for example, in accordance with X.509 and RFC 2459 standards (or
14 other applicable CRL standards) at 312 and at 316 the certificate is formatted (for
15 example, as an ASN.1 or other format CRL.) The digital certificate is signed at 320
16 to assure its authenticity and is then stored at 322 within a computer residing at the
17 Certificate Authority. The process returns at 326. Whenever a request is made for
18 a new digital certificate, process 300 is carried out or, in some instances, the most
19 recently generated CRL may be retrieved and forwarded to the requester.

20 As digital certificates find wider use, the number of such certificates issued
21 has increased dramatically. With this increase comes an associated increase in
22 the number of entries in a Certificate Revocation List. Accordingly, the process 300
23 as just described can become an extremely time consuming process that can
24 result in the CRL being untimely in that many minutes or even hours can pass
25 before an updated CRL can be generated. This is obviously undesirable since the
26 process of authentication using the CRL should preferably be carried out on the
27 most recent information available.

28 In addition to the certificate revocation list just described, certificate
29 authorities commonly generate a certificate revocation list that is referred to as a

delta CRL or Δ CRL. A delta CRL is simply a type of CRL that reflects changes made between two consecutive CRLs. Delta CRLs can be generated, for example, using process 300 wherein the query of 304 is a query that further limits the selection criterion to digital certificates that have been changed since the most recently generated CRL (or between two adjacent CRLs).

The concept of delta CRLs is illustrated in **FIGURE 4** by a sequence of CRLs numbered 1, 2, 3 and 4 with delta CRLs (504, 506 and 508) spanning CRL #1 and CRL #2, CRL #2 and CRL #3, and CRL #3 and CRL #4. With reference to **FIGURE 2**, when a delta CRL is sent at 230, one portion of the processing of the delta CRL at 232 is to retain the data from the most recent CRL while appending the appropriate delta CRL to the existing CRL to update the list of revoked certificates.

SUMMARY OF THE INVENTION

The present invention relates generally to digital certificates and CRLs. Objects, advantages and features of the invention will become apparent to those skilled in the art upon consideration of the following detailed description of the invention.

In one embodiment of the present invention a method and apparatus for producing an enhanced CRL is provided. In response to a request containing an identifier of the most recently owned CRL stored by the requester, a certificate authority generates a CRL spanning from the most recently owned CRL to the current CRL. This CRL is formatted as a delta CRL and transmitted as a reply to the requester. This has the advantage of not requiring transmission of the full CRL even though more than one generation of CRL has occurred since the most recently owned CRL by the requester.

A method of creating a digital certificate revocation list (CRL) consistent with an embodiment of the present invention includes determining a latest owned CRL stored by a CRL recipient; creating a delta CRL comprising a list of digital certificates with a status of satisfying at least one inactive criterion, wherein said

1 status has changed since the latest owned CRL; and sending the delta CRL to the
2 CRL recipient.

3 A method of creating a digital certificate revocation list (CRL) consistent with
4 another embodiment of the invention includes receiving a request for a CRL, the
5 request including an indication of a latest owned CRL; creating a delta CRL
6 comprising a list of digital certificates satisfying at least one inactive criterion since
7 the latest owned CRL; and sending the delta CRL as a reply to the request.

8 A data structure, stored on a computer readable storage medium or
9 transported over an electronic communication medium, for a digital certificate
10 revocation list (CRL) consistent with an embodiment of the invention includes a list
11 of digital certificates representing changes to a CRL that have occurred since
12 generation of at least two additional CRLs. The CRL includes a CRL identifier
13 wherein the CRL is formatted as a delta CRL.

14 The above summaries are intended to illustrate exemplary embodiments
15 of the invention, which will be best understood in conjunction with the detailed
16 description to follow, and are not intended to limit the scope of the appended
17 claims.

19 BRIEF DESCRIPTION OF THE DRAWINGS

20 The features of the invention believed to be novel are set forth with
21 particularity in the appended claims. The invention itself however, both as to
22 organization and method of operation, together with objects and advantages
23 thereof, may be best understood by reference to the following detailed
24 description of the invention, which describes certain exemplary embodiments of
25 the invention, taken in conjunction with the accompanying drawings in which:

26 **FIGURE 1** illustrates a simple exemplary system using digital certificates.

27 **FIGURE 2** is a signal flow diagram describing one use of a digital certificate
28 and certificate revocation list in the system of **FIGURE 1**.

29 **FIGURE 3** is a flow chart describing generation of a CRL.

1 **FIGURE 4** illustrates the generation of delta CRLs.

2 **FIGURE 5** illustrates the generation of delta CRLs spanning multiple delta
3 CRLs.

4 **FIGURE 6** is a signal flow diagram describing use of a delta CRL spanning
5 multiple delta CRLs.

6 **FIGURE 7** is a flow chart describing one method consistent with an
7 embodiment of the present invention for generation of a delta CRL spanning
8 multiple delta CRLs.

9 **FIGURE 8** is a flow chart describing another method consistent with an
10 embodiment of the present invention for generation of a delta CRL spanning
11 multiple delta CRLs.

12 **FIGURE 9** illustrates a computer system suitable for use in conjunction with
13 embodiments of the present invention.

14

15 **DETAILED DESCRIPTION OF THE INVENTION**

16 In the following detailed description of the present invention, numerous
17 specific details are set forth in order to provide a thorough understanding of the
18 present invention. However, it will be recognized by one skilled in the art that the
19 present invention may be practiced without these specific details or with
20 equivalents thereof. In other instances, well known methods, procedures,
21 components, and circuits have not been described in detail as not to unnecessarily
22 obscure aspects of the present invention.

23

24 **NOTATION AND NOMENCLATURE**

25 Some portions of the detailed descriptions which follow are presented in
26 terms of procedures, steps, logic blocks, processing, and other symbolic
27 representations of operations on data bits that can be performed on computer
28 memory. These descriptions and representations are the means used by those
29 skilled in the data processing arts to most effectively convey the substance of their

1 work to others skilled in the art. A procedure, computer executed step, logic block,
2 process, etc., is here, and generally, conceived to be a self-consistent sequence
3 of steps or instructions leading to a desired result. The steps are those requiring
4 physical manipulations of physical quantities.

5 Usually, though not necessarily, these quantities take the form of electrical
6 or magnetic signals capable of being stored, transferred, combined, compared, and
7 otherwise manipulated in a computer system. It has proven convenient at times,
8 principally for reasons of common usage, to refer to these signals as bits, values,
9 elements, symbols, characters, terms, numbers, or the like.

10 It should be borne in mind, however, that all of these and similar terms are
11 to be associated with the appropriate physical quantities and are merely convenient
12 labels applied to these quantities. Unless specifically stated otherwise as apparent
13 from the following discussions, it is appreciated that throughout the present
14 invention, discussions utilizing terms such as "processing" or "querying" or
15 "formatting" or "merging" or "determining" or "receiving" or "requesting" or "signing"
16 or the like, refer to the action and processes of a computer system, or similar
17 electronic computing device, that manipulates and transforms data represented as
18 physical (electronic) quantities within the computer system's registers and
19 memories into other data similarly represented as physical quantities within the
20 computer system memories or registers or other such information storage,
21 transmission or display devices.

22

23 DELTA CRL ENHANCEMENT IN ACCORDANCE WITH THE INVENTION

24 While this invention is susceptible of embodiment in many different forms,
25 there is shown in the drawings and will herein be described in detail specific
26 embodiments, with the understanding that the present disclosure is to be
27 considered as an example of the principles of the invention and not intended to limit
28 the invention to the specific embodiments shown and described. In the description
29 below, like reference numerals are used to describe the same, similar or
30 corresponding parts in the several views of the drawings.

1 As great numbers of digital certificates are issued and revoked, a particular
2 CRL can become extremely lengthy and therefore require substantial amounts of
3 time to transmit, receive and process. The present invention addresses this
4 problem by permitting the generation of a delta CRL that spans multiple
5 generations of CRLs. This is illustrated in **FIGURE 5** wherein, at the request of a
6 requester, a delta CRL can be generated to span multiple CRLs. In this example,
7 a delta CRL 502 is generated to span from CRL #1 to CRL #4. Thus, delta CRL
8 502 contains the certificate revocation list entries of delta CRL 504, delta CRL 506
9 and delta CRL 508.

10 Delta CRL 502 can be created using any number of techniques including
11 simply appending the data from delta CRL 504, 506 and 508 together or by
12 querying a database of digital certificate information for all changes in the
13 certificate revocation list occurring between CRL #4 and CRL #1. The overall
14 process is illustrated by the message flow diagram 600 of **FIGURE 6**. This diagram
15 is similar to message flow diagram 200 of **FIGURE 2** until the point where the
16 remote server requests a CRL of the certification authority. When this occurs at
17 604 of message flow 600, the CRL request includes the number (or other identifier)
18 of the latest CRL owned (stored) by remote server 116. This CRL is designated
19 CRL #L. When the request is received at the certificate authority, a delta CRL is
20 generated that spans CRL #L to the current CRL at 608. This delta CRL is then
21 returned to the remote server at 612 and the remote server processes the delta
22 CRL at 616 by appending its entries to the currently owned CRL #L. This can be
23 literally interpreted to create a new CRL or the data from the delta CRL can simply
24 be appended to the data from CRL #L and used for whatever purpose the CRL is
25 being used for at remote server 116. Once the processing is complete at 516, the
26 remote server now owns an equivalent of the most recent CRL.

27 **FIGURE 7** depicts a process 700 for creation of the delta CRL in accord with
28 the present invention. At 704 the certificate authority or other entity generating the
29 CRL receives a request for a CRL containing the most recent owned CRL (CRL #L).

1 At 708, entries are merged from all delta CRLs between the current CRL and CRL
2 #L to retrieve the data necessary for creation of the delta CRL. This data is then
3 formatted as a delta CRL at 716, signed with a digital signature at 720 and sent to
4 the requester as a reply at 728.

5 In an alternative embodiment, depicted as process 800 of **FIGURE 8**, when
6 a request is received for a CRL, the request containing the most recently owned
7 CRL (CRL #L), a certificate database is queried for the changes taking place
8 between the current state and the state of the most recent CRL at 810. Or, the
9 current CRL (i.e., the most recently generated CRL) itself can be queried to obtain
10 differences between it and CRL #L. This information is then formatted as a delta
11 CRL at 716, signed with a digital signature at 720 and sent as a reply at 728.

12 In this manner, the delta CRL created in accordance with the present
13 invention can be sent as a reply in lieu of sending a complete copy of the most
14 recent CRL which may be much larger in size than the size of several conventional
15 delta CRLs. Thus, transmission timesaving can be achieved as well as processing
16 timesaving.

17 The processes previously described as carried out on a computer system,
18 for example, a computer system residing at the certificate authority 112. Such a
19 computer system is depicted in **FIGURE 9** as 900. Computer system 900 includes
20 a central processor unit (CPU) 910 with an associated bus 915 used to connect the
21 central processor unit 910 to Random Access Memory 920 and Non-Volatile
22 Memory 930 in a known manner. An output mechanism at 940 may be provided
23 in order to display or print output for the computer administrator. Similarly, input
24 devices such as keyboard and mouse 950 may be provided for the input of
25 information from the computer administrator. Computer 900 also may include disc
26 storage 960 for storing large amounts of information such as the list of certificates
27 issued and the most recent Certificate Revocation List as well as any Certificate
28 Revocation List cache and other information as required. Computer system 900
29 is coupled to the network (e.g., the Internet) using a network connection 970 such

1 as an Ethernet adapter coupling computer system 900 through a fire wall and/or
2 locally a network to the Internet.

3 Those skilled in the art will recognize that the present invention has been
4 described in terms of exemplary embodiments based upon use of a programmed
5 processor. However, the invention should not be so limited, since the present
6 invention could be implemented using hardware component equivalents such as
7 special purpose hardware and/or dedicated processors which are equivalents to
8 the invention as described and claimed. Similarly, general purpose computers,
9 microprocessor based computers, micro-controllers, optical computers, analog
10 computers, dedicated processors and/or dedicated hard wired logic may be used
11 to construct alternative equivalent embodiments of the present invention.

12 Those skilled in the art will appreciate that the program steps used to
13 implement the embodiments described above can be implemented using disc
14 storage as well as other forms of storage including Read Only Memory (ROM)
15 devices, Random Access Memory (RAM) devices; optical storage elements,
16 magnetic storage elements, magneto-optical storage elements, flash memory, core
17 memory and/or other equivalent storage technologies without departing from the
18 present invention. Such alternative storage devices should be considered
19 equivalents.

20 The present invention is preferably implemented using a programmed
21 processor executing programming instructions that are broadly described above in
22 flow chart form, and that can be stored in any suitable electronic storage medium
23 or that can be transmitted over any electronic communication medium. However,
24 those skilled in the art will appreciate that the processes described above can be
25 implemented in any number of variations and in many suitable programming
26 languages without departing from the present invention. For example, the order of
27 certain operations carried out can often be varied, and additional operations can be
28 added without departing from the invention. Error trapping can be added and/or
29 enhanced and variations can be made in user interface and information
30 presentation without departing from the present invention. Such variations are

1 contemplated and considered equivalent.

2 While the invention has been described in conjunction with specific
3 embodiments, it is evident that many alternatives, modifications, permutations and
4 variations will become apparent to those skilled in the art in light of the foregoing
5 description. Accordingly, it is intended that the present invention embrace all such
6 alternatives, modifications and variations as fall within the scope of the appended
7 claims.

8 What is claimed is:

9